

**Testimony of Derek Smith**  
**Chairman and Chief Executive Officer, ChoicePoint Inc.**  
**Before the House Energy and Commerce Committee**  
**Subcommittee on Commerce, Trade and Consumer Protection**  
**March 15, 2005**

Chairman Stearns, Representative Schakowsky, and Members of the Committee:

I am Derek Smith, Chairman and Chief Executive Officer of ChoicePoint Inc.

I have thought a great deal, both professionally and as a father, about the role information can play in making our world more, or less, secure. I have devoted the last 12 years to the pursuit of making our society safer through the innovative, but proper, use of technology and information.

At ChoicePoint, our customers cover a broad spectrum of American business, non-profits and government service organizations – from half the Fortune 1000 to notable community organizations, and most of America’s federal, state and local law enforcement agencies.

Last year ChoicePoint helped 100 million American consumers obtain fairly priced home and auto insurance, and thousands of American businesses obtain commercial property insurance. We also helped 8 million Americans get jobs through our workplace pre-

employment screening services. We helped more than one million consumers obtain expedited copies of their vital records – birth, death and marriage certificates.

ChoicePoint helped government fulfill its mission guarding the safety of Americans.

But regretfully, I know that I am not here today to talk only about the good things ChoicePoint has done. I know I am here because your committee and your constituents are concerned about the harm that may have been done to approximately 145,000 Americans, whose information may have fallen into the hands of criminals who accessed ChoicePoint systems.

Let me begin by offering an apology on behalf of our company, as well as my own personal apology, to those consumers whose information may have been accessed by the criminals whose fraudulent activity ChoicePoint failed to prevent.

Beyond our apology, I want to assure the public and the members of this committee that we have moved aggressively to safeguard the information in our possession from future criminal theft. We have also moved promptly to provide assistance to every affected individual to help them avoid financial harm. We also welcome participating in the efforts of this Committee and other policy-makers seeking to provide an appropriate regulation of our industry.

We have decided to exit the consumer sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will no longer sell information products

containing sensitive consumer data including social security and drivers license numbers except where there is a specific consumer driven transaction or benefit or where the products support federal, state or local government and criminal justice purposes. ChoicePoint will continue to provide authentication, fraud prevention and other services to large accredited corporate customers where consumers have existing relationships.

We have strengthened ChoicePoint's customer credentialing process and we are changing our products and services to many customer segments. We are requiring additional due diligence such as bank references and site visits to small business applicants before allowing access to personally identifiable information. We are recredentialing broad sections of our customer base, including our small business customers. We are modifying the services that ChoicePoint is delivering to our customers.

The remaining ChoicePoint products and services that contain sensitive information will satisfy one of three tests:

- Support consumer driven transactions, for which data is needed to complete or maintain relationships such as insurance, employment or tenant screening.
- Provide authentication or fraud prevention tools to large, accredited corporate customers to enable services such as identity verification, customer enrollment or insurance claims.
- Support federal, state or local government and law enforcement purposes.

I have created an office of Credentialing, Compliance and Privacy that will report to our Board of Directors' Privacy Committee and be independent of ChoicePoint management. This office will be based here in Washington and be led by Carol DiBattiste, previously deputy administrator of the Transportation Security Administration and a former senior prosecutor in the Department of Justice with extensive experience in the detection and prosecution of financial fraud.

I have also appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the federal government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials.

These changes reflect some of the lessons we have already learned as a result of the breaches of ChoicePoint's security which have resulted in the recent convictions of several individuals.

From what I now know, on September 27, 2004 a ChoicePoint employee became suspicious while credentialing a prospective small business customer based in the Los Angeles area. This employee brought his concerns regarding the application to our Security Services Department. After a preliminary review, the manager of the Security Services Department alerted the Los Angeles County Sheriff's Department. They decided to initiate an official police investigation and asked for our assistance. That investigation is still ongoing, and has, I am told, already resulted in the arrest and conviction of at least one individual.

After this situation became public last month I learned that another instance in which ChoicePoint had been working with a law enforcement inquiry also involved a criminal use of our information products and, late last year, had resulted in a guilty plea.

With respect to California, we have learned that those involved had previously opened ChoicePoint accounts by presenting fraudulently obtained California business licenses and fraudulent documents. They were then able to access information products primarily containing the following information: consumer names, current and former addresses, social security numbers, driver's license numbers, certain other public record information such as bankruptcies, liens and judgments and, in certain cases, credit reports.

Based on information currently available, we estimate that data from approximately 145,000 consumers may have been accessed as a result of unauthorized access to our information products. Nearly one quarter of those consumers are California residents. California is the only state that statutorily requires affected consumers to be notified of a potential breach of personally identifiable information, and authorizes law enforcement officials to delay notification to allow a criminal investigation to proceed. Last fall, ChoicePoint received such a request from the Sheriff's Department after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time ChoicePoint had not yet reconstructed all of the searches required to identify consumers at risk and law enforcement officers had not yet learned all of the pertinent details of the crime. Working cooperatively with the Sheriff's Department and after

completing the necessary reconstruction, we began the process of notifying consumers last month. We voluntarily elected to use the California law as the basis for notifying consumers in all states. Absent specific notification from law enforcement personnel, affected consumers or others, we can not determine whether a particular consumer has been a victim of actual identity theft. However, law enforcement officials have informed us that they have identified approximately 750 consumers nationwide where some attempt was made to compromise their identity.

The security breach that ChoicePoint discovered last fall in California has caused us to go through some serious soul-searching at ChoicePoint. In retrospect, the company should have acted more quickly. I should have been notified earlier of the investigation being conducted by Los Angeles County Sheriff's Department. What I can tell you today is that from now on, I will be notified when ChoicePoint learns of a formal law enforcement inquiry involving any potential breach of our security.

In the meantime, we have taken other steps to help and protect the consumers who may have been harmed.

- First, ChoicePoint has established a dedicated toll-free customer service number and a special web site to respond to inquiries;
- Second, we are providing, free of charge, a combined three-bureau credit report;
- Third, we are providing, free of charge, a one-year credit monitoring service; and

- For anyone who has suffered actual identity theft from this fraud, ChoicePoint will provide further assistance to help them resolve any issue arising from that identity theft.

We hope these efforts will help those individuals protect their personal data from being used in a criminal manner and that they will mitigate any harm.

Mr. Chairman, I would like to state before this committee, for the record, my position on further regulation or oversight of information and credential verification providers. For the past two years, I have been working to prompt a broad discussion on how we can build a framework that defines how personally identifiable information should be used, by whom and for what purposes. I have called for independent oversight to give the public the confidence it needs. I support increased penalties – criminal penalties – for the unauthorized access to information. I support a single, reasonable, nationwide mandatory notification requirement of any unauthorized access to personally identifiable information.

Every advance in technology that makes our lives easier also makes it easier for our enemies to move swiftly against us. You and I can be approved for a bank account in a matter of minutes, but a person can use that same technology to get a fake or real drivers' license or to create a fake business.

The point being, technology and information are neither good nor bad. People determine if the power of information is used for the benefit of individuals or society or to create harm.

I believe that only by adding a more formal structure to the current scheme of information use, will we realize the full value of technology-based tools to society.

The architects of these guidelines will be working against a backdrop of apparently conflicting principles: increased concerns about privacy balanced against society's need to identify people who would do us harm. But it is important to remember that these two principles are not mutually exclusive, and that too much weight on either end of the spectrum leads not to balance, but to immobility, or worse, to a breaking point. The privacy debate should not be a choice between civil defense and civil liberty. We must aim to preserve both.

Perhaps I might take a few minutes to describe some of the benefits of having access to an individual's personal information. ChoicePoint has helped find more than 800 missing children – we were even able to find a baby kidnapped from a hospital the day he was born, and return him to his parents within 24 hours. Our company works with the largest youth services organizations around the country to help them screen volunteers – we have helped identify more than 11,000 undisclosed felons among those volunteering, or seeking to volunteer. Included in this group, individuals who did not disclose they had been convicted of a collective 5176 violent crimes, 1137 sex crimes, 11,397 illegal

substance offenses, 1055 crimes against children. Forty-two of these individuals were registered sex offenders.

ChoicePoint's DNA laboratories have freed those wrongly accused from prison, and helped to identify suspects and victims of violent crimes. Our labs matched thousands of bone fragments found in the World Trade Center rubble with DNA samples provided by victims' families. Our scientists are currently in the tsunami ravaged areas of Asia helping to identify victims to help bring closure to families devastated by the disaster.

ChoicePoint helped Maryland police identify and locate two men named John Allen Muhammad and Lee Boyd Malvo. The two had no obvious relationship to one another and no known ties to Washington, DC. Information technology found those hidden links, and provided the tools for locating the people now known as the DC Snipers.

In fact, ChoicePoint provides service to more than 7,000 federal, state and local law enforcement agencies.

Not all of what we do is so dramatic. ChoicePoint also serves 700 insurance companies, a large number of Fortune 500 companies, and many large financial services companies. And the products involved in these transactions are regulated by the FCRA, which represents a significant portion of our business. Certain other segments of our business are regulated by Gramm-Leach-Bliley Act and various state laws.

We look forward to participating in continued discussion of these issues, and I pledge our cooperation to your efforts.

I thank you for your consideration, and I would be pleased to answer any questions you might have.

# # #